- **Control Temporary PINs**

  When adding a new subscriber to the VMS, the system administrator should assign a randomly generated 6-digit temporary PIN. The system administrator should have sole responsibility for the preparation and control of these temporary PINs.

- **Periodically Change All PINs**

  Change each mailbox PIN every 30 days—or at least every 90 days. The VMS should be modified to allow automatic system prompting of callers to change their PINs. There is a natural reluctance on the part of the callers to follow through with this necessary action, but it should be required.

- **Remove All Unassigned Mailboxes**

  All unassigned mailboxes should be removed from the system. Mailboxes left unassigned for months are an invitation to the criminal element.

- **Remove Unused Mailboxes**

  Set a deadline for how long mailboxes can be left unused—and then deactivate the boxes. Ideally, the deadline should be 30 days—and never longer than 90 days. Mailboxes assigned to former employees, summer interns, or to current employees who no longer have access to the system should be deactivated immediately. To make these changes as soon as possible, system administrators should stay directly in touch with your company's personnel department.

- **Set a Deadline for Initiating Mailboxes**

  Set a time limit—such as one week—to activate newly assigned mailboxes. If not activated within that time, mailboxes should be removed from service.

- **Do Not Publish Remote Access Numbers**

  If possible, do not publish the remote access telephone number. This is an invitation to thieves.

- **Terminate Access After Third Invalid PIN Attempt**

  You should limit attempts at entering the VMS PIN. Just modify system software ("kill" software) to terminate a call automatically after a third invalid attempt—or route the call to an attendant. A simple disconnect should show up in the daily review of system audit trails, but transferring the call to an attendant will often deter potential thieves and provide real-time detection of possible fraud. Attendants should keep a log of this activity; and if a number of these attempts occur in a short period of time, they should notify the VMS system administrator.

- **Restrict Out Dialing**

  If the VMS is connected to a PBX, remove all out-dial applications within the VMS.

This prevents thieves from entering through a remote access local telephone number—or 800 service. Once they enter the system, they can manipulate the VMS and PBX systems to gain access to the company's long-distance trunks and local direct dial capability.

Most VMSs come with an auto attendant function, which usually has a "verify extension" field capability. The 9XXX field should be blocked to prohibit all out-dial capabilities. If "8" is used for all "0+" dialing capabilities, then the 8XXX field should also be blocked. If possible, program the PBX to block all VMS access trunks and local direct dial capabilities using the PBX's facility restriction levels. Or consider restricting the outbound VMS trunk line with the following restrictions. They include "1+", "0+", "0-", "00+", "00-", 976, 950, 411, 611, and 10XXX numbers and any other restrictions your system may be capable of. Requests to the vendor should be put in writing, with a copy saved.

If you need the local direct dial capability, try to block the 91XXX, 90XXX and 80XXX (if used for 0+ dialing) fields within the auto attendant function ("verify extension field" capability). If possible, program the PBX to block all VMS access to the PBX's long-distance trunks—using PBX facility restriction levels. Or consider restricting the outbound VMS trunk line with the same restrictions listed above and any other restrictions your system may be capable of.

If you need the local *and* long-distance direct dial capabilities, then you should assign alternate facility restriction levels for non-business hours. Set up these restrictions within the PBX to block all VMS access to the PBX's long-distance trunks—and local direct dial capabilities. Consider the restrictions outlined in the paragraphs above and any other restrictions your system may be capable of.

If your PBX's restriction capabilities are limited, look into Pacific Bell *Centrex*. *Centrex* trunks can establish **all** of the restrictions outlined above. For more information about Pacific Bell *Centrex*, turn to Chapter 9, or contact your Pacific Bell Account Executive.

If your VMS is in a stand-alone configuration—or provided by a local telephone company affiliate or other off-premises provider—it is usually connected to your local telephone company's switching network through *Centrex* lines. If you do not need long-distance service and local direct dial access, you should remove all out-dialing applications within the VMS. Or you can restrict the system's auto attendant feature by obtaining *Toll Restriction* through your *Centrex* lines. To limit outbound dialing further, restrict call transfers—so they remain within the *Centrex* (4- or 5-digit dialing).

If you only need local "direct-dial" capability, see if you can block "1+", "0+", "0-", "00+", "00-", 976, 950, 411, and 611 capability in the VMS, and any other restrictions your system may be capable of. And try to restrict 10XXX casual calling and outbound 800 access during non-business hours.

- **Limit Your 800 Number**

  If you use 800 service for remote access to the VMS, limit that service to the geographical area your company really needs. For instance, if you do business only in the western United States, do not purchase eastern access. Another inexpensive defense against toll fraud is to include Call Detail Reports as part of your 800 service. Then review usage patterns often to watch for signs of fraud. Pacific Bell *Custom* 800 Call Detail Reports include the full 10 digits of the calling number, and is provided as a free service. Pacific Bell *Custom* 800 also has features that allow you to receive incoming calls only from select area codes and/or specific prefixes.

- **Guard Against Voice Mail "Squatters"**

  Criminals need a safe location where they can dependably exchange information. They often penetrate VMSs, take over inactive boxes for months, and exchange information regarding drugs, pornography, prostitution, and other stolen access numbers and codes.

  In a specific case in California, criminals took over an entire VMS. And in another case, thieves threatened a system administrator who discovered their penetration—explaining that they must be allowed to use their "safe" voice mailboxes, or they would take over the entire system. According to reports, this type of extortion is not unique, and some system administrators have agreed to such demands rather than confront those who penetrated the system. However, this type of agreement will only lead to other problems, including potential legal liabilities. Instead, system administrators should routinely monitor for "squatters" and root them out. If threatened, the administrator should immediately contact both the local law enforcement agency and the Secret Service.

- **Use Effective System Audit Trails**

  System administrators are responsible for the overall integrity of their VMSs—as well as preventing unauthorized access to mailboxes. To accomplish these goals, they should:

  – Monitor system audit trails on a regular basis to effectively manage the system.

  – Monitor system reports for excessive after-hours use, unsuccessful PIN attempts, unusual out-dialing patterns, and a reduction in system storage capacity.

  – Check all active mailboxes to ensure they belong only to current employees or customers.

  – Obtain Call Detail Reports from their 800 service provider for each 800 group.

  – Look for an unusual increase in 800 line usage and the name associated with the caller's billing number.

  – Monitor SMDR data and trunk activity reports, for systems with an out-dialing capability.

- Respond to complaints from employees and customers about the VMS. Include an immediate investigation of complaints of messages not being received, customers being locked out of the system (i.e., PIN changed), and obscene messages or altered greetings appearing in selected mailboxes.

- **Load Only Randomly Generated Data File Lists**

  Do not allow vendors to load the same data file lists of active mailboxes into newly installed systems. Vendors should use randomly generated lists for this purpose.

- **Guard Against Collect Call Schemes**

  1 Recently, three new voice mail schemes have surfaced. In the first scheme, a thief accesses an unused mailbox in a VMS and leaves a message in the mailbox authorizing the acceptance of collect calls. The thief then calls the mailbox collect and accesses the VMS.

  2 In the second scheme, the thief places a collect call to an unused mailbox. When the operator requests authorization to accept the collect call, the thief responds. The operator, unable to distinguish between the thief and the called party, puts the call through.

  3 With the third scheme, the thief places a collect or third-party call to a number associated with a VMS. The interactive voice response (IVR) system unintentionally accepts charges from the electronic operator used in many pay phones. On a collect call, the pay phone electronic operator says, "I have a collect call; if you will not accept a collect call, hang up." Since the IVR is programmed to respond to a voice, it replies—effectively accepting the collect or third-party call. The IVR's owner is then charged for the call. This is an increasing problem and very popular among prisoners. In all cases, if the VMS is unprotected, the thief can then gain access to the entire system, and place outgoing calls.

  To avoid these problems, use a software feature known as *Billed Number Screening** from Pacific Bell which tells the carrier's operator that collect and third-party billed calls are not permitted from that number. This service is frequently used by hospitals and other institutions.

- **Educate Employees About VMS Toll Fraud**

  Employees should be instructed to safeguard their VMS PINs and not share their unique PIN codes with anyone. They should be warned about indicators that could signal a fraudulent incident in progress, e.g., messages not being received, employees and customers being locked out of their mailboxes, obscene messages, or altered greetings appearing in selected mailboxes. They should be instructed to notify their system administrators as soon as possible after these or other unusual situations occur.

* *When processing third-number and collect calls, some carriers do not use or access Pacific Bell's database containing the billing restrictions described. Therefore, it is possible for unauthorized third-number and collect calls to appear on your bill.*

VOICE MAIL SYSTEM TOLL FRAUD INDICATORS

Operational VMS Toll Fraud Indicators

- Staff or customer complaints of an inability to enter the system.
- Any indication that the system is "clogged" or overloaded.
- Messages not being received.
- Unexplained problems related to being "locked out" of the system or PIN changes.
- Altered greetings.
- Obscene messages.
- Unusual increases in data storage volume.

Statistical VMS Fraud Indicators

- VMS initiated calls through a PBX. These calls are characterized by an unusual extension code in the extension data field.
- Any VMS indicators that are abnormal, including excessive non-business hour use, unusual out-dialing patterns, reduction in system storage capacity.

CALL DIVERTER TOLL FRAUD

A call diverter is a device used to forward calls to another location, usually after regular business hours. A call diverter typically requires the use of two exchange lines: an incoming line to receive calls and an outgoing line to transfer calls. The user directs the call diverter to transfer all incoming calls to a predetermined number. Call diverters are widely used, with well over a million such systems in operation. Calls are normally diverted to an answering service, a user's 24-hour work center, or to an employee's home. Call diverters are particularly popular with businesses and professionals that receive calls after normal hours.

Long-distance thieves call a user's published telephone number after normal business hours to determine if and how the call is diverted. If the call is diverted and answered, the intruders pretend to have misdialed or they remain silent. When the called party hangs up, the call diverter sometimes leaves a momentary dial tone before the disconnect. When this happens, the thief seizes the dial tone and uses it to place long-distance telephone calls. In most cases, the company that owns the call diverter does not know this has occurred until it receives the next month's telephone bill. If you employ such a system, the actions listed below should be taken to protect against this type of toll fraud.

- **Modify the Call Diverter**

  Contact the vendor to request inspection and modification of your call diverter. The vendor should ensure that connection to the outgoing line is immediately disconnected if a secondary dial tone appears. If you buy a new call diverter system, have this inspection and modification completed before you activate the system. However, not all call diverters can be modified to detect secondary dial tone. Your vendor will know what is possible for your system.

- **Convert to Pacific Bell Call Forwarding**

  You can use Pacific Bell *Call Forwarding* and *Delayed Call Forwarding* to forward calls from an individual's telephone number to another pre-selected number. This can replace your call diverter and does not allow access to secondary dial tone.

- **Set Toll Restrictions on Outgoing Lines**

  If you use a call diverter with a PBX or *Centrex*, be sure to use toll restrictions on the outgoing line. Restrict the line to local access only and block all "0+" and "1+" calls. You should also consider restricting "0-", "00+", "00-", 976, 411, 611, 950, 10XXX, as well as the number of long-distance trunks—and any other restrictions your system is capable of.

- **Employ Billed Number Screening**

  You can request Pacific Bell to place *Billed Number Screening** on incoming lines. With this feature, third-number billed or collect calls cannot be charged to an incoming line.

- **Take Call Diverters Out of Numerical Sequence**

  When multiple call diverters have their telephone numbers in numerical sequence —for example, 1520, 1521, 1522, etc.—it is easier for intruders to identify the call diverters. Be sure to change this numerical sequence, contacting Pacific Bell to reassign telephone numbers on a random basis.

- **Educate Employees About Call Diverter Toll Fraud**

  Educate all employees—including answering service personnel—about the risk of call diverter toll fraud. They should be alerted to watch for fraud indicators, such as frequent wrong numbers or silence on the line.

OPERATIONAL CALL DIVERTER TOLL FRAUD INDICATORS

- A sudden increase in calls from parties that claim to have "misdialed."
- A sudden increase in the number of "dead" or "open" lines.
- A sudden increase in usage and activity.

* *When processing third-number and collect calls, some carriers do not use or access Pacific Bell's database containing the billing restrictions described. Therefore, it is possible for unauthorized third-number and collect calls to appear on your bill.*

Chapter 5

AUTO ATTENDANT TOLL FRAUD

An auto attendant is a device that can be incorporated into either a PBX or VMS. It answers the phones for the company, welcomes the customer, and asks the caller to press the number of the desired extension. It usually advises the caller to press zero to obtain operator assistance if the extension number is not known.

Long-distance thieves enter the auto attendant function through a local telephone line or 800 service. When asked to enter the desired extension, they enter 91XX, 90XX, 80XX, 81XX. The auto attendant attempts to transfer to that extension, which to many PBXs and VMSs (with out-dialing capabilities) signifies an outgoing long-distance call. Once the auto attendant dials the requested numbers, the intruders dial the balance of digits necessary to place long-distance phone calls. Toll fraud through an auto attendant is a serious and growing problem. To lessen your risk, we suggest you take the actions listed below.

AUTO A + PBX

- **Auto Attendant/PBX Configuration**

  The auto attendant capability usually has a "verify extension field" capability. The 9XXX field should be blocked to prohibit all out-dialing capabilities. If "8" is used for all "0+" dialing capabilities, then the 8XXX field should also be blocked. If possible, the access lines between the auto attendant and the PBX should be toll-restricted using PBX facility restriction levels. This includes "1+", "0+", "0-", "00+", "00-", 976, 611, 411, 950, 10XXX, etc., and any other restrictions your system is capable of. Also make sure that the outgoing trunk group codes are made unavailable from the auto attendant.

AUTO A + PBX + VMS

- **Auto Attendant/VMS Configuration—With VMS Connected to the PBX**

  If your VMS is integrated with a PBX, remove all out-dialing capabilities within the VMS. The 9XXX field within the auto attendant—or "verify extension field" capability—should be blocked, prohibiting all out-dialing capabilities. If "8" is used for all "0+" dialing capabilities, then the 8XXX field should also be blocked. If possible, block all VMS access to the PBX long-distance trunks and local direct dial capabilities using the PBX's facility restriction levels. This includes "1+", "0+", "0-", "00+", "00-", 976, 611, 411, 950, 10XXX, etc., and any other restrictions your system is capable of.

  If you need a local out-dialing capability for the VMS, then see if you can block the 91XX, 90XX, and 8XXX (if used for "0+" dialing) fields within the "verify extension field" capability of the auto attendant function. If possible, block all VMS access to the PBX long-distance trunks and local long-distance capabilities using PBX facility restriction levels. This includes "1+", "0+", "0-", "00+", "00-" restrictions.

If you need local *and* long-distance out-dialing capabilities, then you should assign alternate facility restriction levels for non-business hours. Set up these restrictions within the PBX to block all VMS access to the PBX long-distance trunks—and local long-distance direct dial capabilities. Consider the restrictions outlined in the paragraphs above and any other restrictions your system may be capable of.

If you are not able to make these changes yourself, contact your vendor for assistance. If these restrictions cannot be obtained through your vendor, contact Pacific Bell to see about *Centrex* and its associated toll restriction capabilities. (See Chapter 9 for details on *Centrex* features.)

- **Auto Attendant/VMS Configuration (Stand-Alone)**

  If the VMS stands alone, it is usually connected to Pacific Bell's network through *Centrex* lines. If you do not require long-distance service and local direct dial access, be sure to remove all out-dialing capabilities within the VMS. As an added protective measure, obtain *Toll Restriction* through *Centrex* (including the restrictions outlined above) and *Billed Number Screening** from Pacific Bell.

  If you need local out-dialing capability, see if you can block "1+", "0+", "0-", "00+", "00-" in the VMS. And obtain *Toll Restriction* ("1+", "0+", and "0-") on your *Centrex* lines and *Billed Number Screening** from Pacific Bell.

  If you need local *and* long-distance out-dial capability, obtain appropriate *Toll Restriction* ("1+", "0+", "0-", "00+", "00-") on your *Centrex* line and *Billed Number Screening** from Pacific Bell. If possible, restrict casual dialing (10XXX), as well as 976, 950, 411, 611, etc.

* *When processing third-number and collect calls, some carriers do not use or access Pacific Bell's database containing the billing restrictions described. Therefore, it is possible for unauthorized third-number and collect calls to appear on your bill.*

Chapter 6

CPE PORT TOLL FRAUD

System administration ports allow the system administrator—or vendor representatives—to access the PBX or VMS so they can perform routine tasks. These include administrative and maintenance functions involved in managing the system's software and hardware—such as the administration of PBX and voice mail trunks, terminals, and features.

These access ports are sometimes referred to as "maintenance ports." They provide the ability to generate system reports on all communications facilities and services—as well as the ability to detect, report, and correct system hardware and software problems quickly. Many telecommunications systems also have ports that allow the control of various environmental features, such as climate control or lighting systems. Unfortunately, each separate port configuration or capability can also be penetrated by long-distance thieves. These ports are becoming extremely popular with hackers and are quite vulnerable.

A very high percentage of CPE owners do not even realize their systems have maintenance and system administration ports. As a result, they do not take adequate steps to protect these ports from being used by thieves of long-distance service.

In almost all cases, we recommend that these ports be totally deactivated. They are usually equipped with an on/off switch, which should be disabled—unless *authorized* users require access for a specific task. Upon completion of the task, the switch should *immediately* be disabled again. Contact your vendor for technical assistance in blocking or deactivating these ports.

When a PBX or VMS is shipped by the vendor, it contains start-up or default accounts, passwords, and permissions installed at the factory. These accounts, passwords, and permissions provide the vendor with full system privileges. Some common default accounts are "backup," "field," "service," etc. Commonly used passwords can be 1-2-3-4-5, 5-4-3-2-1, etc. Long-distance service thieves are well aware of these simple codes. Be sure to eliminate the data before you activate the equipment.

Perpetrators of toll fraud can often enter a company's PBX or VMS through system administration ports and vendor-provided default accounts, passwords, and permissions. In fact, if criminals obtain full system privileges, they can remotely reprogram the PBX or VMS to provide capabilities not previously activated. For example, a company may leave the DISA function in a PBX inactive as a way of avoiding toll fraud. But the hacker can activate the DISA function remotely, and the company will remain unaware of this penetration and calling activity. In a VMS, criminals can take over the entire system, deny authorized customers or employees access to the system, establish new mailboxes, sell stolen mailboxes, or read confidential corporate messages between employees. The following actions can help protect PBX and VMS system administration and maintenance ports from toll fraud.

1
- **Activate Ports Manually—Deactivate Automatically**

  For all remote access system administration ports, use manual procedures to activate the port—and deactivate automatically. Physically disconnect remote access lines to your system administration ports—until the system administrator has verified the authorization of any organization seeking access.

  You can physically disconnect the remote access capability for such system ports. Just contact your vendor, if you are unsure how to accomplish this. Be sure to take this step for all CPE, and deactivate their ports. If the vendor calls with a good reason to use the ports, it's easy to activate them temporarily—then *promptly deactivate* them when the procedure has been completed.

2
- **Randomly Select System Administration Port Telephone Numbers**

  Telephone extension numbers for system administration ports should be randomly selected. Do not use predictable extension numbers such as X500, X600, etc.

3
- **Delete Vendor Default Accounts, Passwords, and Permissions**

  Many systems operate for months or years with original default or password codes—such as 1-2-3-4—which can be easily penetrated. Delete all vendor-provided default accounts, passwords, and permissions from VMS or PBX systems. When a vendor requires access to the system for administration or maintenance purposes, provide a randomly generated temporary password. Once the temporary password has been used, delete it from the system. Then, issue a new temporary password each time the vendor requires access to the system. In addition, see what happens to your password if your system fails or you shut it down. Some systems revert to the factory default password when this occurs—without alerting the system administrator to the change.

4
- **Use Smart Modems**

  Use smart modems on all remote access system administration ports. A fixed call-back modem is the most effective dial-access security tool available. However, consider whether your situation warrants the variable call-back or password-connection mode. Options include:

  - **Fixed Call-Back Modem**

    The fixed call-back modem associates the telephone number in its database with a password and identification (ID) pair. The modem enters both the password and ID and disconnects the line. Then it calls the distant party back, before linking the caller to the PBX or VMS. The distant party must use the same password and ID needed for log-on—and must call from the same location. Since the distant-end party is using a dialing or inbound modem for qualifying authorized access, no physical connection between the answering modem and the PBX or VMS is made. Even if long-distance service thieves obtain the password and ID, they still are not able to enter the system because the modem calls back the authorized user at a pre-established number. There are two disadvantages to this type of modem: The owner of the system must pay for the call-back, and the remote party must operate from a fixed location.

  - **Variable Call-Back Modem**

    The variable call-back modem prompts the distant-end caller for the phone number at their current location—which can be transient. Then it calls back to that location. Although this system can be defeated, it does record the call-back number used by the distant-end party. So, if a hacker uses the call-back modem to penetrate a system, the system administrator obtains the hacker's telephone number.

  - **Password Connection Security Modem**

    The password connection security modem provides a high degree of security, but it is somewhat difficult to administer. The password is stored in two locations: in the modem at the PBX or VMS location—and in the modem used by the distant-end party. When the modem connection is made, the passwords are exchanged. If they do not match, the connection is aborted. The PBX or VMS system administrator controls password assignments and can change passwords in the distant-end modem remotely from the PBX location.

  - **Use the Maximum Number of Digits for Codes**

    Assign the maximum number of digits allowable for all access authorization codes and barrier codes. Most systems can handle between 12 and 15 digits. The greater the number of digits used, the greater the protection. Temporary system administrator codes used for vendor remote interface should have the same maximum number of digits as permanent access authorization codes.

  For additional security, you could have separate *Direct Inward Dial* (DID) trunks from Pacific Bell to the modem—and then return or dial-back on a *Direct Outward Dial* (DOD) trunk only. Or you could use Pacific Bell *Select Call Acceptance* for an added level of security. This feature limits access by allowing only predetermined numbers to call in to the modem.

- **Use Multiple Levels of Security Access**

  Wherever possible, use multiple levels of security access for VMS or PBX system administration ports.

- **Randomly Generate All Codes**

  All access authorization codes should be randomly generated by the user's system administrator—avoiding consecutive numbers or sequential codes. The codes should then be reviewed by either the system administrator or an independent third party, to reject codes that are particularly susceptible to penetration.

- **Periodically Change All Codes**

  Change each access authorization code every 30 days—or *at least* every 90 days.

- **Deactivate All Unassigned Codes**

  Have your system administrator maintain an independent log of all permanent and temporary access authorization codes, and keep the log in a secure place. Then review the codes regularly—and deactivate any unused codes.

- **Terminate Access at the Third Invalid Attempt**

  Modify the system's PBX and VMS software to automatically terminate access after the third invalid attempt. When an invalid attempt occurs, the software should alert the PBX operator, VMS attendant, or the appropriate system administrator

CPE PORT TOLL FRAUD INDICATORS

- A sudden and unexplained inability to access specific administrative functions.
- An inability to retrieve calling data.
- An unusual increase in PBX or voice mail memory usage.
- Any unexplained changes in system software parameters.
- Any unusual maintenance or administrative port activities.
- Any indications that there may have been unauthorized access authorization code assignments.

Chapter 7

PAGER TOLL FRAUD

With the growing use of "beepers" and pagers, the problem of pager toll fraud is on the rise too. Pagers are a primary tool of thieves who set up shady operations disguised as pay-call (dial-it) services—then profit from the highly responsive habits of employees who use pagers.

Here's how the scheme works: The thieves set up a pay-call service, using a telephone company that does not limit the rate that can be charged for the service. Then they obtain lists of beeper/pager numbers—and dial hundreds of calls to these numbers every day. When the pager users respond and hear the pay-call message, they generally assume they have misdialed or some other mistake has been made. The thieves then bill the employees' companies for the call—and about 80 percent of the time, the companies pay without questioning the charges.

Thieves often use "976 look-a-like" exchanges as part of this fraud, since the numbers are not generally recognized as toll calls. (These exchanges are used in cities where the 976 exchange cannot accommodate further service.) Then, when unsuspecting employees return calls to these numbers, their companies are charged.

Refer to pages 18–19 for a list of "976 Look-A-Like" numbers.

Chapter 8

PROSECUTING THE CULPRITS

Pacific Bell offers support for toll fraud prevention and quick intervention. These important approaches help prevent the need for prosecution—which is generally a last resort. That's because criminal prosecution requires significant activity and involvement from victims. These activities include: filing complaints, writing reports, signing affidavits, meeting with detectives, and testifying before the Grand Jury.

When the long-distance carrier or local telephone company is the victim, these important responsibilities are delegated to experienced security professionals employed by the carrier. They are familiar with the criminal justice procedures required to prosecute the perpetrators—and can handle associated details quickly and efficiently. When a toll fraud victim is a customer and owner of CPE, all of these responsibilities fall on a bookkeeper, telecommunications manager, or a company executive with little or no knowledge or experience in investigation or litigation of toll fraud. In that case, the victim is often discouraged and frustrated by the complicated steps necessary for prosecution. The combination of time, commitment, costs, and frustration often results in a decision to drop the criminal prosecution effort.

Toll fraud is a high-tech and computer-intensive crime, requiring law enforcement agencies to develop levels of expertise equal to or greater than that of the criminal subcultures. The nature of the crime makes it exceedingly difficult to track down and apprehend those involved. One cannot "arrest" a pay phone. Often, a toll fraud incident is referred to law enforcement weeks or months after the fact. By then, the criminal is long gone, preying on other victims.

A number of problems associated with prosecuting toll fraud criminal cases are not present in the prosecution of other crimes. For example, the way this crime is perpetrated makes it difficult to trace and prove. And there are many criminals involved in the chain of events leading to toll fraud:

- **The hacker,** who illegally obtains and sells access code information—and who can easily dump this information in seconds. This erases all evidence of their existence and the hacker's involvement.

- **The middleman,** who purchases the access code information and sells it on the street to drug dealers or parties interested in "selling" calls. Simple possession of an access code is not illegal, and these codes are frequently encoded when sold.

- **The numerous actual users of access codes.** Since codes are widely distributed and used at pay phones—by many callers—it becomes difficult to trace and prosecute each individual user.

It is commonly believed that hackers and long-distance service thieves are never prosecuted and never go to jail. That is incorrect. There have, in fact, been numerous successful prosecutions—with significant numbers of individuals now serving jail terms, in both federal and state correctional systems. And there are persistent efforts by law enforcement to combat this fraud. Law enforcement officials are successful as they overcome the problems of tracking and apprehending the perpetrator—and acquire greater technical expertise.

In the event you are victimized, contact your local law enforcement agency and your long-distance carrier. Also notify your Pacific Bell Account Executive or call the Fraud Hotline at 1-800-953-5366. Experienced consultants and investigators can assist you—and can help determine whether the perpetrators can be identified and prosecuted to the full extent of the law.

Chapter 9

PACIFIC BELL LockOn IS YOUR ASSURANCE OF PROTECTION AGAINST TELEPHONE TOLL FRAUD

When you see the *LockOn* symbol, you know that Pacific Bell is working to protect you from toll fraud. Toll fraud affects businesses like yours every day. Today in California, many businesses are having long-distance phone calls stolen from them.

Whether you have a Pacific Bell *Centrex*, a Key System or PBX, your business may be vulnerable to toll fraud—unauthorized calls made through your telephone system. You may be paying for someone else's phone calls!

With *LockOn*, Pacific Bell has taken a proactive role in helping to provide customers with safeguards against toll fraud. And where toll fraud has occurred, we're working hard to prevent its recurrence.

Pacific Bell *LockOn* is the service that can help you secure your communications system against toll fraud. *LockOn* is provided to all Pacific Bell customers at no charge, and protects in four ways: prevention, detection, intervention, and prosecution.

Prevention

Pacific Bell can provide information on toll fraud, how it occurs and how it can be prevented. In addition, Pacific Bell can provide you with a risk assessment of your specific network configuration and a report on what can be done to make your system more secure. For an appointment, call your Pacific Bell Account Team Representative.

Detection and Intervention

Centralized Fraud Bureau

Centralized Fraud Bureau team members continually monitor the system for warning signals connected to specifically set thresholds. When our network surveillance service detects fraudulent calling patterns, the customer's Pacific Bell Account Team is alerted or the customer is alerted directly.

- Early alert programs monitor Pacific Bell's billing records for fraudulent calling patterns and alert the Centralized Fraud Bureau as early as 6 hours after a fraudulent calling pattern begins.
- Pacific Bell receives Fraud Hotline tips from employees, customers, and long-distance carriers.

- Network specialists review early warning reports and refer suspected remote access fraud to the bureau's team of fraud specialists.
- The bureau's fraud specialists confer with the customer, the Pacific Bell Account Team, central office technical support, the CPE vendor, and others to secure the customer's system and resolve the problem.
- After an incident of toll fraud has been discovered and action taken to halt the fraud, Pacific Bell continues to monitor the system to ensure that corrective measures are effective and that the fraud doesn't recur after a brief lapse of time.

PROSECUTION

In cases where a suspect can be identified, Pacific Bell will work with local law enforcement agencies, the FBI, the Federal Secret Service, and other relevant agencies to prepare the evidence for successful prosecution under state and federal laws.

PLEASE BE SURE THAT PACIFIC BELL HAS A CURRENT NUMBER AT WHICH AN EMPLOYEE FAMILIAR WITH YOUR TELECOMMUNICATIONS EQUIPMENT CAN BE REACHED EVENINGS, WEEKENDS, OR ON HOLIDAYS IN THE EVENT OF AN EMERGENCY.

To contact Pacific Bell or the Centralized Fraud Bureau call the Fraud Hotline: 1-800-953-5366.

Leave a detailed message, including a number where you can be reached, and a team member will respond.

Chapter 10

CENTREX - FRAUD PREVENTION

If you have Pacific Bell *Centrex*, you can minimize your risk of remote access fraud. Using *Centrex* lines with dialing restrictions instead of regular business lines or trunks provides you with important defenses against fraud. *Centrex* offers a variety of features to control dialing access at every level—from intra-system only (no outside calls can be dialed) to restricted area codes and prefixes. Pacific Bell also offers backup features that will alert you to fraud, in case your first line of defense is penetrated.

The following *Centrex* features will help to minimize your losses—with little or no inconvenience:

- **Station Restrictions**

  Pacific Bell *Centrex* comes with standard selective dialing treatments for each station. Each station is configured for *Originating and Terminating Restrictions. Terminating Restrictions* will differentiate and control internal and external termination to a station. *Originating Restrictions* include: local only, local and ZUM, 7- and/or 10-digit intraLATA toll, "0+", "0-", interLATA toll or international dialing—and any combination of these, all or none.

- **Toll Diversion**

  In conjunction with *Station Restrictions*, an optional feature, *Toll Diversion* will allow the system administrator to selectively block specific area codes and/or prefixes.

- **Automatic Route Selection-Deluxe**

  Like *Toll Diversion*, *Automatic Route Select-Deluxe* will block the completion of numbers with specific area code and/or prefixes, but it also provides least-cost routing for all authorized system users. It does this by comparing the user dialing privileges with the number dialed, selecting the least-cost facility as determined by the customer for the completion of authorized calls, and by blocking unauthorized calls.

- **Authorization Codes**

  Authorization Codes allow an individual to complete a call for which the station would otherwise be blocked (either by *Station Restrictions* or *Automatic Route Selection-Deluxe*). *Authorization Codes* are assigned to individuals and can be selectively invoked based on the dialing privileges of the calling station. When attempting to dial an otherwise blocked call, the user is prompted to enter up to a 15-digit authorization code that is verified by the switch's database. If the dialing privileges of the authorization code are equal to or greater than those of the called number, the call will be completed. If less, the call is blocked.

- **Select Call Acceptance**

  Select Call Acceptance automatically accepts calls from up to 31 user-selected telephone numbers. Calls from other numbers are blocked from terminating on a line where *Select Call Acceptance* is activated.

  Where *Select Call Acceptance* is activated, it will block unauthorized callers to PBX DISA lines, dial-up modems or fax machines. Only callers whose telephone number matches one on the list will be able to complete their calls.

  Callers may be forwarded to another number or receive an announcement that the called party is not accepting their call. Forwarding the caller to another line with *Select Call Acceptance* will create an effective list size of 155 by chaining five lines together.

- **Station Message Detail Recording to Premises**

  Station Message Detail Recording to Premises (SMDR-P) delivers real-time Call Detail Reports—records generated by station users to the users' premises. In addition to its traditional use to provide bill-back and facility operational status, it can be used to detect any misuse of your system. Because SMDR-P provides a record of each call at its completion, it can be used to perform analysis to identify any system violation, if one should occur. System administrators should watch for multiple short-duration incoming calls and long-duration outgoing calls. They should monitor PBX activity at off-peak hours such as evenings and weekends. Particular attention should be given to international long-distance calls. System administrators should also look for multiple failed attempts to access the PBX or multiple calls to unusual locations.

Chapter 11

TOLL FRAUD PREVENTION CHECKLISTS

The number of businesses being hit by toll fraud is growing steadily. And the cost of these incidents is soaring. But you can prevent these costly losses and discourage those who are taking advantage of business telephone systems. The following checklists have been developed to help minimize your risk of toll fraud. Carefully consider each of the sections that apply to your telephone system, and take whatever action is necessary to protect your system from becoming the target of toll fraud.

The checklists that follow are:

- PBX Toll Fraud
- Voice Mail Toll Fraud
- Call Diverter Toll Fraud
- Auto Attendant Toll Fraud
- CPE Port Toll Fraud

PBX TOLL FRAUD PREVENTION CHECKLIST

	YES	NO	DON'T KNOW
• Have you evaluated the necessity of using the remote access feature (DISA) and use it only if necessary?	( )	( )	( )
• If DISA is not needed, have you asked your vendor to block or eliminate the feature?	( )	( )	( )
• Are you using the maximum number of digits for all access authorization codes and barrier codes, preferably 15?	( )	( )	( )
• Are your access authorization codes and barrier codes randomly generated? This would preclude consecutive number or sequential codes, and using codes equivalent to: – Telephone extension numbers. – Employee identification numbers. – Social security numbers. – Anniversaries. – Maiden names. – First names.	( )	( )	( )
• Does the system administrator issue security codes?	( )	( )	( )
• Has the system administrator ensured that each employee has a separate and distinct access code?	( )	( )	( )
• Have group or department access codes been eliminated?	( )	( )	( )
• Are there multiple levels of security for both barrier and access codes?	( )	( )	( )
• Are your authorization codes and barrier codes changed periodically, monthly if possible, and never to exceed 90 days of use between changes?	( )	( )	( )
• Have all unassigned access authorization codes been deactivated?	( )	( )	( )

PBX TOLL FRAUD PREVENTION CHECKLIST *cont.*

	YES	NO	DON'T KNOW
• Does the system administrator keep an independent authorized users and their access log of all authorization codes?	( )	( )	( )
– Does the system administrator compare codes in the PBX with the log at least monthly, and correct all discrepancies immediately?	( )	( )	( )
• Have all codes not being used by authorized employees been deactivated?	( )	( )	( )
• Has the remote access telephone number been published?	( )	( )	( )
– If it has, have steps been taken to issue a new number?	( )	( )	( )
• Has the PBX software been programmed to terminate access after a third invalid barrier code or access authorization code attempt?	( )	( )	( )
– Has the software been modified to automatically terminate a call or route to an attendant?	( )	( )	( )
• Do you restrict or block remote access capability during non-business hours?	( )	( )	( )
– Use time-of-day restriction feature.			
– Use automatic route selection feature.			
• Have you ensured the 800 number servicing the remote access feature has the correct geographic band?	( )	( )	( )
– Restrict to only the area codes required.			
– Purchase Call Detail Reports for each 800 number.			
• Have you eliminated a steady-state dial tone as a remote access prompt?	( )	( )	( )
– Use a voice recording or silent prompt.			
– Use a ring delay option. Wait four or five rings before the answer connection is made.			